



IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s) Richard Paul TARQUINI et al.

Confirmation No.: 7297

Application No.: 10/003,510

Examiner: Zia, Syed

Filing Date: 10/31/2001

Group Art Unit: 2131

Title: METHOD AND COMPUTER-READABLE MEDIUM FOR INTEGRATING A DECODE ENGINE
WITH AN INTRUSION DETECTION SYSTEM

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on August 31, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

() (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

() one month	\$120.00
() two months	\$450.00
() three months	\$1020.00
() four months	\$1590.00

() The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$500.00. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: 10/31/2005

OR

() I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number _____ on _____

Number of pages:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

Richard Paul TARQUINI et al.

By: James L. Baudino
James L. Baudino

Attorney/Agent for Applicant(s)

Reg. No. 43,486

Date: 10/31/2005

Telephone No.: (214) 855-7544



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

In re Application of: Richard Paul TARQUINI et al.
Serial No.: 10/003,510
Filing Date: October 31, 2001
Group Art Unit: 2131
Examiner: Zia, Syed
Title: METHOD AND COMPUTER-READABLE MEDIUM
FOR INTEGRATING A DECODE ENGINE WITH
AN INTRUSION DETECTION SYSTEM
Docket No.: 10017331-1

MAIL STOP: APPEAL BRIEF PATENTS
Commissioner for Patents)
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Applicants has appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed July 14, 2005, finally rejecting Claims 1-16. Applicants filed a Notice of Appeal on August 31, 2005. Applicants respectfully submits herewith this Appeal Brief with authorization to charge the statutory fee of \$500.00.

11/04/2005 DTESSEM1 00000109 082025 10003510

01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on March 18, 2002 Assignment Records of the United States Patent and Trademark Office at Reel 012717, Frame 0691. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-16 stand rejected pursuant to a Final Office Action mailed July 14, 2005. Claims 1-16 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a method of detecting network-intrusions at a first node (270A-270N) of a network (100) comprising identifying a frame as an intrusion by an intrusion detection application (91, 110), archiving event-data associated with the frame, and decoding the event-data by a decode engine (430), the decode engine (430) integrated within the intrusion detection application (91, 110). (at least at page 10, line 24 to page 11, line 27; page 13, line 12 to page 14, line 5; page 14, line 16 to page 15, line 4; page 17, line 1 to page 18, line 11; and figures 2-7).

Embodiments of the present invention as defined by independent Claim 10 are directed toward a computer-readable medium having stored thereon a set of

instructions to be executed, the set of instructions, when executed by a processor (272), cause the processor (272) to perform a computer method of identifying, by an intrusion detection application (91, 110), a frame of data as intrusion-related, and decoding, by the intrusion detection application (91, 110), the intrusion-related data. (at least at page 10, line 24 to page 11, line 27; page 12, lines 11-30; page 13, line 12 to page 14, line 5; page 14, line 16 to page 15, line 4; page 17, line 1 to page 18, line 11; and figures 2-7).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claim 10 was rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,704,874 issued to Porras (hereinafter "*Porras*").
2. Claims 1-9 and 11-16 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Porras* and further in view of U.S. Patent No. 6,453,345 issued to Trcka et al. (hereinafter "*Trcka*").

ARGUMENT

A. Standard

1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim

limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. Claims 1-9

Claims 1-9 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Porras* and in view *Trcka*. Of the rejected claims, Claim 1 is independent. Applicants respectfully submit that independent Claim 1 is patentable over the cited references, and thus remaining Claims 2-9 which depend from independent Claim 1 are also patentable.

Embodiments of the present invention generally involve a method for detecting network intrusions. For example, according to one embodiment of Applicants' invention, a network node (270A-270N) is configured to run an instance of an intrusion prevention system (IPS) application (91) implemented as a three-layered IPS (at least at page 14, lines 16-18). In this embodiment of Applicants' invention, the network node (270A-270N) comprises a network protocol stack (90) having a transport driver interface (TDI) (125), a transport driver (130), a protocol driver (135) and a media access control (MAC) driver (145) that interfaces with a physical media (101) page 17, lines 1-11; and figures 3 and 4). Embodiments of Applicants' invention incorporate a decode application (450) having a decode engine

(430) into an IPS application service provider (110), also referred to as an IPS server, of the IPS application (91) (at least at page 17, lines 12-16; page 18, lines 12-29; and figures 6 and 7). In some embodiments of Applicants' invention, the decode engine (430) comprises logic for interpreting raw network data, such as binary streams of a network frame captured off an Ethernet, and converting the network data into a format suitable for viewing and for facilitating analysis thereof by a network manager or security personnel (at least at page 18, lines 12-29; and figures 6 and 7). For example, decode engine (430) is configured to distinguish between a plurality of network protocols and parse packets of captured network frames and provide interpretations of specific parts thereof (at least at page 18, lines 12-29; and figures 6 and 7). The event-data decoded by the decode engine (430) is then provided to an event viewer application (410) and/or a report server application (420) (at least at page 18, line 30 to page 19, line 7; and figures 6 and 7). Accordingly, Applicants' Claim 1, for example, recites "identifying a frame as an intrusion by an intrusion detection application," "archiving event-data associated with the frame" and "decoding the event-data by a decode engine, the decode engine integrated within the intrusion detection application."

In the Final Office Action, the Examiner relies on a monitoring system 22 of *Porras* as corresponding to "identifying a frame as an intrusion by an intrusion detection application" recited by Claim 1, and a translation module 32 of *Porras* as corresponding to "decoding the event-data by a decode engine" as recited by Claim 1 (Final Office Action, page 6). The Examiner also appears to assert that such translation module 32 of *Porras* is "integrated within the intrusion detection application" as is required by Applicants' Claim 1 (Final Office Action, page 6). Applicants respectfully disagree.

Porras appears to disclose a monitoring system 22 having, for example, an intrusion detection system (*Porras*, column 3, lines 30-32, figure 1). *Porras* recites:

Each of the [monitoring systems] 22 monitor various host and/or network activity within the networks 12-16, and each [monitoring system] 22, as discussed above, generate a stream of alerts, triggered by potentially

suspicious events, such as network packet data transfer commands, data transfer errors, network packet data transfer volume, and so forth. The alerts indicate a suspicion of possible malicious intrusion or other threat to operations within the networks 12-16.

(*Porras*, column 3, lines 54-61). *Porras* also appears to disclose that the monitoring system 22 of *Porras* sends the above-referenced alert stream via a secure electronic communication line (SSL) 30 to an alert manager 24 for collection, processing and distribution (*Porras*, column 3, lines 34-37, lines 62-67, figure 1). *Porras* appears to disclose that the alert manager 24 of *Porras* is equipped with a translation module 32 to translate original, raw data streams received from the monitors 22 into a common format for further processing (*Porras*, column 4, lines 6-10). Referring especially to figure 1 of *Porras*, the alert manager 24 and translation module 32 of *Porras* are separate and apart from the monitoring system 22 of *Porras*. In fact, *Porras* clearly indicates that the translation module 32 of *Porras* receives an alert stream via a secure electronic communication line (SSL) from the monitoring system 22 of *Porras* (*Porras*, column 3, lines 34-37, lines 62-67, figure 1). Thus, the translation module 32 of *Porras* relied on by the Examiner is not “integrated within” the monitoring system 22 of *Porras* as is required by Applicants’ Claim 1 (emphasis added). To the contrary, the Examiner relies on the monitoring system 22 of *Porras* as corresponding to the “intrusion detection application” recited by Claim 1 but offers no support or showing that the translation module 32 of *Porras* relied on by the Examiner as corresponding to the “decode engine” recited by Claim 1 is “integrated within” the monitoring system 22 of *Porras*. Moreover, *Trcka* does not remedy the above-referenced deficiencies of *Porras*, nor has the Examiner relied on *Trcka* to teach the above-referenced deficiencies of *Porras* or as a motivation to combine *Trcka* with *Porras*. Accordingly, for at least these reasons, Claim 1 is patentable over the cited references. Therefore, Applicants respectfully submit that the rejection of Claim 1, and Claims 2-9 that depend therefrom, was improper and that Claims 1-9 are in condition for allowance.

2. Claims 10-16

Claim 10 was rejected under 35 U.S.C. §102(e) as being anticipated by *Porras*. Claims 11-16 were rejected under 35 U.S.C. §103(a) as being unpatentable

over *Porras* and in view *Trcka*. Of the rejected claims, Claim 10 is independent. Applicants respectfully submit that independent Claim 10 is patentable over the cited reference, and thus remaining Claims 11-16 which depend from independent Claim 10 are also patentable.

In the Final Office Action, the Examiner relies on the monitoring system 22 of *Porras* as corresponding to “identifying, by an intrusion detection application, a frame of data as intrusion-related” recited by Claim 10, and a translation module 32 of *Porras* as corresponding to “decoding, by the intrusion detection application, the intrusion-related data” as recited by Claim 10 (emphasis added) (Final Office Action, page 5). Applicants respectfully disagree.

As discussed above on connection with independent Claim 1, *Porras* appears to disclose that the monitoring system 22 of *Porras* includes an intrusion detection system for monitoring various host and/or network activity and generating a stream of alerts triggered by potentially suspicious events or malicious intrusions within the networks 12-16 of *Porras* (*Porras*, column 3, lines 30-32 and 54-61). *Porras* also discloses that the generated stream of alerts are sent via a secure electronic communication line (SSL) 30 to an alert manager 24 for collection, processing and distribution, and that the alert manager 24 of *Porras* is equipped with a translation module 32 to translate original, raw data streams received from the monitors 22 into a common format for further processing (*Porras*, column 3, lines 34-37 and 62-67; column 4, lines 6-10; and figure 1). Claim 10 recites “identifying, by an intrusion detection application, a frame of data as intrusion-related” and “decoding, by the intrusion detection application, the intrusion-related data” (emphasis added). The Examiner relies on the monitoring system 22 of *Porras* as corresponding to the “intrusion detection application” recited by Claim 10 but offers no support or showing that such monitoring system 22 of *Porras* “decod[es] . . . the intrusion-related data” as is required by Applicants’ Claim 10. To the contrary, the Examiner relies on the remote translation module 32 of *Porras* for supplying such “decoding,” yet the translation module 32 of *Porras* clearly is not part of the monitoring system 22 of *Porras*. Nor does the Examiner rely on *Trcka* to teach the above-referenced deficiencies of *Porras* or as a motivation to combine *Trcka* with *Porras* for either


independent Claim 10 of Claims 11-16 that depend from independent Claim 16. Accordingly, Applicants respectfully submit that the rejection of Claim 10, and Claims 11-16 that depend therefrom, was improper and that Claims 10-16 are in condition for allowance.

CONCLUSION

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of \$500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,


James L. Baudino
Registration No. 43,486

Date: 10/31/05

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884

CLAIMS APPENDIX

1. A method of detecting network-intrusions at a first node of a network, comprising:

identifying a frame as an intrusion by an intrusion detection application;

archiving event-data associated with the frame; and

decoding the event-data by a decode engine, the decode engine integrated within the intrusion detection application.

2. The method according to claim 1, further comprising providing, by a network filter service provider of the intrusion detection application, the event-data to an event-database.

3. The method according to claim 2, further comprising providing the event-data to a decode server.

4. The method according to claim 3, wherein the decode server obtains the event-data from at least one of an event viewer and a report server.

5. The method according to claim 1, further comprising:

generating a report from the decoded event-data; and

providing the report to a report viewer.

6. The method according to claim 1, further comprising providing, by the intrusion detection application, the decoded event-data to an intrusion detection client application.

7. The method according to claim 6, wherein the decoded event-data is formatted, by the client application, for display in a graphical user interface.

8. The method according to claim 6, wherein the intrusion detection application runs locally on the first node.

9. The method according to claim 6, wherein the intrusion detection client application runs remotely on a second node, the first node and the second node operable to engage in a communication session between the client application and the intrusion detection application.

10. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

identifying, by an intrusion detection application, a frame of data as intrusion-related; and

decoding, by the intrusion detection application, the intrusion-related data.

11. The computer-readable medium according to claim 10, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of generating a report from the decoded intrusion-related data.

12. The computer-readable medium according to claim 10, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of archiving the decoded intrusion-related data in a database.

13. The computer-readable medium according to claim 10, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of archiving the identified data in a database.

14. The computer-readable medium according to claim 11, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of transmitting the decoded data to a client application.

15. The computer-readable medium according to claim 14, wherein transmitting the decoded data to a client application further comprises transmitting the report to a client application in communication with the intrusion detection application.

16. The computer readable medium according to claim 15, wherein transmitting the report to a client application further comprises transmitting the report to the client application in communication with the intrusion detection application, the client application running remotely from the intrusion detection application.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None